

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Samuel H. Christie, IV

Examiner: Sherkat, Arezoo

Serial No. 09/650,120

Art Unit: 2131

Filed: 08/28/2000

For: **FIREWALL CONTROL FOR SECURE PRIVATE NETWORKS WITH PUBLIC VoIP ACCESS**

Mail Stop Appeal Brief – Patents

Commissioner for Patents

PO Box 1450

Alexandria, VA 22313-1450

Sir:

An **APPEAL BRIEF** is filed herewith. Appellant also encloses a payment in the amount of \$1520.00 to cover the fees associated with a Three-month Extension of Time and with this appeal brief as required by 37 C.F.R. § 1.17(c). If any additional fees are required in association with this appeal brief, the Director is hereby authorized to charge them to Deposit Account 50-1732, and consider this a petition therefor.

APPEAL BRIEF

(1) REAL PARTY IN INTEREST

The real party in interest is the assignee of record, i.e., Nortel Networks Limited of 2351 Boulevard Alfred-Nobel, St. Laurent, Quebec Canada H4S 2A9, which is wholly owned by Nortel Networks Corporation, a Canadian corporation.

(2) RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences to the best of Appellant's knowledge. A notice of appeal was filed in this case on February 24, 2005, but Appellant reopened prosecution by filing a Request for Continued Examination.

(3) STATUS OF CLAIMS

Claims 1-29 were rejected with the rejection made final on June 7, 2006.

Claims 1-29 are pending.

Claims 1-29 are the subject of this appeal.

(4) STATUS OF AMENDMENTS

All amendments have been entered to the best of Appellant's knowledge. No amendments have been made after the final rejection mailed June 7, 2006.

(5) SUMMARY OF CLAIMED SUBJECT MATTER

The invention relates to a method of remotely controlling a firewall from a firewall controller in order to permit the flow of packet data through the firewall (Specification, page 4, lines 5-8). The firewall controller can be a call server in a VoIP telephony system such as a media gateway controller (*Id.* at page 4, lines 8-10). The method includes having the firewall controller determine the need for a pinhole in the firewall. This occurs when a media gateway endpoint on the secure side of the firewall either wishes to place a call to an endpoint outside the firewall or receive a call from an endpoint outside the firewall. Both of these events are made known to the media gateway endpoint's call server. The firewall controller sends a request to the firewall requesting that a pinhole be opened for a specific address pair corresponding to the respective media gateway endpoints involved in the call. The firewall carries out the request and opens a pinhole. Upon termination of the call, the firewall controller determines that the pinhole is no longer needed and sends a request to the firewall to close the pinhole. The firewall then closes the pinhole (*Id.* at page 4, lines 10-24).

In particular, claim 1 recites a method of remotely controlling a firewall (see Figure 2, firewall 225) from a firewall controller (such as Figure 2, media gateway controller 205) in order to permit the flow of packet data through said firewall (Specification, page 4, lines 5-8), the method comprising:

- sending a request message from a firewall controller to a firewall requesting that a pinhole be opened (Specification, page 4, lines 17-20; page 12, lines 4-10; page 13, lines 15-20; see also Figure 3, step 310)

- opening a pinhole in said firewall (Specification, page 4, lines 20-21; page 12, lines 7-10; page 13, lines 20-22; see also Figure 3, step 315)

- sending a request message from a firewall controller to said firewall requesting that a pinhole be closed (Specification, page 4, lines 21-24; page 12, lines 15-17; page 14, lines 1-2; see also Figure 3, step 335); and

closing said pinhole (Specification, page 4, line 24; page 12, lines 17-18; page 14, lines 2-3; see also Figure 3, step 340).

Claim 8 is similar to claim 1 but is from the point of view of the firewall controller. In particular, claim 8 recites a firewall controller (such as Figure 2, media gateway controller 205) for permitting the flow of packet data, said firewall controller comprising:

means (such as Figure 2, media gateway controller 205) for determining a need for a pinhole in a firewall (Figure 2, firewall 225)(Specification, page 10, line 28 through page 11, line 2; see also Figure 3, step 305);

means (such as Figure 2, media gateway controller 205) for sending a request message to said firewall requesting that a pinhole be opened in said firewall (Specification, page 4, lines 17-20; page 12, lines 4-10; page 13, lines 15-20; see also Figure 3, step 310); and

means (such as Figure 2, media gateway controller 205) for sending a request message to said firewall requesting that said pinhole be closed in said firewall (Specification, page 4, lines 21-24; page 12, lines 15-17; page 14, lines 1-2; see also Figure 3, step 335).

Claim 12 recites a firewall (Figure 2, firewall 225) responsive to a firewall controller (such as Figure 2, media gateway controller 205) for permitting the flow of packet data, said firewall comprising:

means (pinhole filter in firewall 225, see Specification, page 2, lines 1-12; page 13, lines 20-24; see also Figure 3, steps 315 and 320) for receiving a request message from said firewall controller requesting that a pinhole be opened in said firewall (Specification, page 4, lines 17-20; page 12, lines 4-10; page 13, lines 15-20; see also Figure 3, step 310);

means (pinhole filter in firewall 225, see Specification, page 2, lines 1-12; page 13, lines 20-24; see also Figure 3, steps 315 and 320) for opening a pinhole in said firewall (Specification, page 4, lines 20-21; page 12, lines 7-10; page 13, lines 20-22; see also Figure 3, step 315);

means (pinhole filter in firewall 225, see Specification, page 2, lines 1-12; page 13, lines 20-24; see also Figure 3, steps 315 and 320) for receiving a request message from said firewall controller requesting that said pinhole be closed in said firewall (Specification, page 4, lines 21-24; page 12, lines 15-17, page 14, lines 1-2; see also Figure 3, step 335); and

means (pinhole filter in firewall 225, see Specification, page 2, lines 1-12; page 13, lines 20-24; see also Figure 3, steps 315 and 320) for closing said pinhole in said firewall

(Specification, page 4, line 24; page 12, lines 17-18; page 14, lines 2-3; see also Figure 3, step 340).

Claim 15 recites a firewall (Figure 2, firewall 225) responsive to a media gateway controller (such as Figure 2, media gateway controller 205) for permitting the flow of packet data, said firewall comprising:

means (pinhole filter in firewall 225, see Specification, page 2, lines 1-12; page 13, lines 20-24; see also Figure 3, steps 315 and 320) for receiving a request message from said media gateway controller requesting that a pinhole be opened in said firewall (Specification, page 4, lines 17-20; page 12, lines 4-10; page 13, lines 15-20; see also Figure 3, step 310);

means (pinhole filter in firewall 225, see Specification, page 2, lines 1-12; page 13, lines 20-24; see also Figure 3, steps 315 and 320) for opening a pinhole in said firewall (Specification, page 4, lines 20-21; page 12, lines 7-10; page 13, lines 20-22; see also Figure 3, step 315);

means (pinhole filter in firewall 225, see Specification, page 2, lines 1-12; page 13, lines 20-24; see also Figure 3, steps 315 and 320) for receiving a request message from said media gateway controller requesting that said pinhole be closed in said firewall (Specification, page 4, lines 21-24; page 12, lines 15-17, page 14, lines 1-2; see also Figure 3, step 335); and

means (pinhole filter in firewall 225, see Specification, page 2, lines 1-12; page 13, lines 20-24; see also Figure 3, steps 315 and 320) for closing said pinhole in said firewall (Specification, page 4, line 24; page 12, lines 17-18; page 14, lines 2-3; see also Figure 3, step 340).

Claim 16 recites a computer program product (see Specification, page 14, line 22 through page 16, line 17) for remotely controlling a firewall (Figure 2, firewall 225) from a firewall controller (such as Figure 2, media gateway controller 205) in order to permit the flow of packet data through said firewall, the computer program product having a medium with a computer program embodied thereon, the computer program product comprising:

computer program code in said firewall controller for sending a request message to said firewall requesting that a pinhole be opened (Specification, page 4, lines 17-20; page 12, lines 4-10; page 13, lines 15-20; see also Figure 3, step 310); and

computer program code in said firewall for opening a pinhole (Specification, page 4, lines 20-21; page 12, lines 7-10; page 13, lines 20-22; see also Figure 3, step 315);

computer program code in said firewall controller for sending a request message to said firewall requesting that said pinhole be closed (Specification, page 4, lines 21-24; page 12, lines 15-17; page 14, lines 1-2; see also Figure 3, step 335); and

computer program code in said firewall for closing said pin hole (Specification, page 4, line 24; page 12, lines 17-18; page 14, lines 2-3; see also Figure 3, step 340).

Claim 21 recites a computer program product (Specification, page 14, line 22 through page 16, line 17) in a firewall controller (such as Figure 2, media gateway controller 205), said firewall controller operative with a firewall (Figure 2, firewall 225), the computer program product having a medium with a computer program embodied thereon, the computer program product comprising:

computer program code for determining the need for a pinhole in said firewall (Figure 2, firewall 225)(Specification, page 10, line 28 through page 11, line 2; see also Figure 3, step 305);

computer program code for sending a request message to said firewall requesting that a pinhole be opened in said firewall (Specification, page 4, lines 17-20; page 12, lines 4-10; page 13, lines 15-20; see also Figure 3, step 310); and

computer program code for sending a request message to said firewall requesting that said pinhole be closed in said firewall (Specification, page 4, lines 21-24; page 12, lines 15-17; page 14, lines 1-2; see also Figure 3, step 335).

Claim 25 recites a computer program product (Specification, page 14, line 22 through page 16, line 17) in a firewall (Figure 2, firewall 225), said firewall responsive to a firewall controller (such as Figure 2, media gateway controller 205), the computer program product having a medium with a computer program embodied thereon, the computer program product comprising:

computer program code for receiving a request message from said firewall controller requesting that a pinhole be opened in said firewall (Specification, page 4, lines 17-20; page 12, lines 4-10; page 13, lines 15-20; see also Figure 3, step 310);

computer program code for opening a pinhole in said firewall (Specification, page 4, lines 20-21; page 12, lines 7-10; page 13, lines 20-22; see also Figure 3, step 315);

computer program code for receiving a request message from said firewall controller requesting that said pinhole be closed in said firewall (Specification, page 4, lines 21-24; page 12, lines 15-17, page 14, lines 1-2; see also Figure 3, step 335); and

computer program code for closing said pinhole in said firewall (Specification, page 4, line 24; page 12, lines 17-18; page 14, lines 2-3; see also Figure 3, step 340).

Claim 26 recites a computer program product (Specification, page 14, line 22 through page 16, line 17) in a firewall (Figure 2, firewall 225), said firewall responsive to a media gateway controller (such as Figure 2, media gateway controller 205), the computer program product having a medium with a computer program embodied thereon, the computer program product comprising:

computer program code for receiving a request message from said media gateway controller requesting that a pinhole be opened in said firewall (Specification, page 4, lines 17-20; page 12, lines 4-10; page 13, lines 15-20; see also Figure 3, step 310);

computer program code for opening a pinhole in said firewall (Specification, page 4, lines 20-21; page 12, lines 7-10; page 13, lines 20-22; see also Figure 3, step 315);

computer program code for receiving a request message from said media gateway controller requesting that said pinhole be closed in said firewall (Specification, page 4, lines 21-24; page 12, lines 15-17, page 14, lines 1-2; see also Figure 3, step 335); and

computer program code for closing said pinhole in said firewall (Specification, page 4, line 24; page 12, lines 17-18; page 14, lines 2-3; see also Figure 3, step 340).

Claim 27 recites a computer system for remotely controlling a firewall (Figure 2, firewall 225) from a firewall controller (such as Figure 2, media gateway controller 205) comprising:

a firewall (Figure 2, firewall 225) operatively connected to a private computer network (private network of Figure 2) and at least one external computer network (such as public network in Figure 2);

a firewall controller (such as Figure 2, media gateway controller 205) operatively connected to said firewall for remotely instructing said firewall to open and close pinholes in said firewall (Specification, page 4, lines 5-20; page 12, lines 4-24; page 13, line 15 through page 14, line 3; see also Figure 3).

Claims 4, 11, 20, and 24 are argued separately. Each of these claims recites "wherein said firewall controller is a media gateway controller" (see Figure 2, media gateway controller 225).

(6) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Whether claims 1-3, 5, 8, 12, 15-17, 21, 25, and 26 were properly rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,631,416 B2 to Bendinelli et al. (hereinafter “Bendinelli”).¹

B. Whether claims 4, 6, 9, 11, 13, 18, 20, 22, 24, and 27-29 were properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Bendinelli in view of U.S. Patent Application Publication No. 2002/0120760 A1 to Kimchi et al. (hereinafter “Kimchi”).

C. Whether claims 7, 10, 14, 19, and 23 were properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Bendinelli in view of U.S. Patent No. 6,611,864 B2 to Putzolu et al. (hereinafter “Putzolu”).

(7) ARGUMENT

A. Introduction

The present invention and each of the independent claims relate to providing direct communications between a firewall and a firewall controller, such that the firewall controller can send requests to open and close pinholes in the firewall. The benefit of the invention lies in its ability to dynamically manage a pinhole in a private network firewall, such that VoIP communications between endpoints on the private network and endpoints on a network beyond the firewall do not compromise the security of the private network (Specification, page 3, lines 11-15). In particular, the present invention avoids using protocol specific proxies, which use an alternate path into the secure private network, as pointed out by Appellant in the background of the invention (Specification, page 3, lines 3-7).

Claims 1-3, 5, 8, 12, 15-17, 21, 25, and 26 all contain limitations regarding a firewall controller sending requests to a firewall to open and close pinholes through the firewall. Claims 4, 11, 20, 24, and 26 specify that the firewall controller is a media gateway controller. Bendinelli does not teach a firewall controller sending requests to a firewall to open and close pinholes through the firewall. Instead, Bendinelli uses an alternate proxy, referenced as a proxy module 1520, to provide an alternate path into the private network, which is exactly what the present

¹ The Patent Office nominally rejected claims 1-29 under 35 U.S.C. § 102(e) as being anticipated by Bendinelli (see Final Office Action mailed June 7, 2006, bottom of page 4). However, in the body of the rejection, the Examiner only rejects claims 1-3, 5, 8, 12, 15-17, 21, 25, and 26 under 35 U.S.C. § 102(e) as being anticipated by Bendinelli. *Id.* at pages 5-6. The remaining claims are rejected under 35 U.S.C. § 103(a) as being obvious over Bendinelli in combination with a secondary reference. *Id.* at pages 6-10.

invention is trying to avoid (see Specification, page 3, lines 3-7). In Bendinelli, there are no direct communications between a firewall controller and a firewall. Instead, the proxy module 1520 coordinates with the respective gateways, 1510 or 1530, to bypass the respective firewalls. Bendinelli specifically states that proxy module 1520 is used as a hairpin, thereby bypassing the firewall 1591 of the second gateway 1530 (Bendinelli, col. 39, lines 1-7). Thus, Bendinelli does not teach a firewall controller sending requests to a firewall to open and close pinholes through the firewall, as does the claimed invention. The Patent Office admits that Bendinelli does not teach where the firewall controller is a media gateway controller, but instead relies on a reference to the media gateway control protocol in Kimchi to allegedly teach that element. Kimchi discloses media gateway controllers, but does not teach or suggest using media gateway controllers as firewall controllers. Thus, Kimchi does not cure the deficiencies of Bendinelli. Likewise, Putzolu also fails to teach the limitations missing from Bendinelli.

Accordingly, since the references alone or in combination, fail to teach or suggest each and every element of the claimed invention, pending claims 1-29 are allowable. As such, Appellant requests that the Board reverse the Examiner and instruct the Examiner to allow the claims for these reasons.

B. Summary of the References

1. U.S. Patent No. 6,631,416 B2 to Bendinelli

Bendinelli is directed to a method and system for enabling a tunnel between two computers on a network. An additional processor is used to enable a network between a first and a second processor (Bendinelli, Abstract). The additional processor may receive information indicating a consent on behalf of the first processor and the second processor to enabling a tunnel between the first and second processors. The additional processor determines a first virtual address for the first processor and a second virtual address for the second processor, such that the first and second virtual addresses uniquely identify the first and second processors, respectively, and are routable through the network. *Ibid.* The additional processor may then provide to each of the first and second processors the first and second virtual addresses to enable one or more tunnels between the first and second processors. *Ibid.* In one embodiment of Bendinelli, an alternate proxy, referenced as a proxy module 1520, is used to provide an alternate path into the private network (Bendinelli, Figures 15A and 15B; see also col. 38, line 59 through col. 41, line

9). There are no direct communications between a firewall controller and a firewall. Instead, the proxy module 1520 coordinates with the respective gateways, 1510 or 1530, to bypass the respective firewalls, 1590 or 1591. In particular, Bendinelli specifically states that proxy module 1520 is used as a hairpin, thereby "...bypassing the firewall 1591 of the second gateway 1530" (Bendinelli, col. 39, lines 1-7). Similar operation is provided for the embodiment illustrated in Figure 15B of Bendinelli.

2. U.S. Patent Application Publication No. 2002/0120760 A1 to Kimchi

Kimchi relates to a robust HTTP based multiple function protocol (Kimchi, paragraph 0003). The protocol is used between subscriber clients and a server-based communication system (Kimchi, Abstract). At the lowest level, the protocol uses HTTP as a transport, and a combination of a URL format and content-information to describe intent and results. *Ibid.* The protocol is transactional in nature and follows a pattern; that is, the client sends a request, and the server replies. *Ibid.*

3. U.S. Patent No. 6,611,864 B2 to Putzolu

Putzolu is directed to a policy based network management system. The method includes sending a first message from a policy enforcement point (PEP) to a policy decision point (PDP) in response to an external action, and sending a Java object in a second message from the PDP to the PEP in response to receiving the first message. The Java object may be executed on the PEP to implement a policy (Putzolu, Abstract).

C. Legal Standards

1. The Standards for Establishing Anticipation

Section 102 of the Patent Act provides the statutory basis for an anticipation rejection and states *inter alia*:

A person shall be entitled to a patent unless

(e) the invention was described in - (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for the

purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language. . . .

The Federal Circuit's test for anticipation has been set forth numerous times. "It is axiomatic that for prior art to anticipate under 102 it has to meet every element of the claimed invention." *Hybritech Inc. v. Monoclonal Antibodies, Inc.*, 802 F.2d 1367, 1379 (Fed. Cir. 1986). This standard has been reinforced. "To anticipate a claim, a reference must disclose every element of the challenged claim and enable one skilled in the art to make the anticipating subject matter." *PPG Indus. Inc. v. Guardian Indus. Corp.*, 75 F.3d 1558, 1577 (Fed. Cir. 1996) (citations omitted). Further, "a finding of anticipation requires that the publication describe all of the elements of the claims, arranged as in the patented device." *C.R. Bard Inc. v. M3 Sys. Inc.*, 157 F.3d 1340, 1349 (Fed. Cir. 1998) (emphasis added and citations omitted).

2. The Standards for Establishing Obviousness

Section 103(a) of the Patent Act provides the statutory basis for an obviousness rejection and reads as follows:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Courts have interpreted 35 U.S.C. § 103(a) as a question of law based on underlying facts. As the Federal Circuit stated:

Obviousness is ultimately a determination of law based on underlying determinations of fact. These underlying factual determinations include: (1) the scope and content of the prior art; (2) the level of ordinary skill in the art; (3) the differences between the claimed invention and the prior art; and (4) the extent of any proffered objective indicia of nonobviousness.

Monarch Knitting Mach. Corp. v. Sulzer Morat GmbH, 45 U.S.P.Q.2d (BNA) 1977, 1981 (Fed. Cir. 1998) (internal citations omitted).

Once the scope of the prior art is ascertained, the content of the prior art must be properly combined. Initially, the Patent Office must show that there is a suggestion to combine the references. *In re Dembiczak*, 175 F.3d 994 (Fed. Cir. 1999). Even if the Patent Office is able to

articulate and support a suggestion to combine the references, it is impermissible to pick and choose elements from the prior art while using the application as a template. *In re Fine*, 837 F.3d 1071 (Fed. Cir. 1988). To reconstruct the invention by such selective extraction constitutes impermissible hindsight. *In re Gorman*, 933 F.2d 982 (Fed. Cir. 1991). After the combination has been made, for a *prima facie* case of obviousness, the combination must still teach or fairly suggest all of the claim elements. *In re Royka*, 490 F.2d 981 (C.C.P.A. 1974); MPEP § 2143.03.

While the Patent Office is entitled to give claim terms their broadest reasonable interpretation, this interpretation is limited by a number of factors. First, the interpretation must be consistent with the specification. *In re Hyatt*, 211 F.3d 1367, 1372 (Fed. Cir. 2000); MPEP § 2111. Second, the broadest reasonable interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach. *In re Cortright*, 165 F.3d 1353, 1359, (Fed. Cir. 1999); MPEP § 2111. Finally, the interpretation must be reasonable. *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1369 (Fed. Cir. 2004); MPEP § 2111.01. This means that the words of the claim must be given their plain meaning unless Appellant has provided a clear definition in the specification. *In re Zletz*, 893 F.2d 319, 321 (Fed. Cir. 1989).

If a claim element is missing after the combination is made, then the combination does not render obvious the claimed invention, and the claims are allowable. As stated by the Federal Circuit, “[if] the PTO fails to meet this burden, then the Appellant is entitled to the patent.” *In re Glaug*, 283 F.3d 1335, 1338 (Fed. Cir. 2002).

D. Claims 1-3, 5, 8, 12, 15-17, 21, 25, and 26 Are Not Anticipated by Bendinelli

Claims 1-3, 5, 8, 12, 15-17, 21, 25, and 26 were rejected under 35 U.S.C. § 102(e) as being anticipated by Bendinelli. For a reference to be anticipatory, the reference must disclose each and every claim element. Further, the elements of the reference must be arranged as claimed. MPEP § 2131. The requirement that each and every element be disclosed in the manner claimed is a rigorous standard that the Patent Office has not met in this case.

As stated above in the summary of the claimed subject matter, the present invention and each of the independent claims relate to providing direct communications between a firewall and a firewall controller, such that the firewall controller can send requests to open and close pinholes in the firewall. The benefit of the invention lies in its ability to dynamically manage a pinhole in a private network firewall, such that VoIP communications between endpoints on the

private network and endpoints on a network beyond the firewall do not compromise the security of the private network (Specification, page 3, lines 11-15). In particular, the present invention avoids using protocol specific proxies, which use an alternate path into the secure private network, as pointed out by Appellant in the background of the invention (Specification, page 3, lines 3-7).

For example, claim 1 recites that the following steps involving communications between a firewall and a firewall controller:

- sending a request message from a firewall controller to a firewall requesting that a pinhole be opened;
- opening a pinhole in said firewall;
- sending a request message from a firewall controller to said firewall requesting that a pinhole be closed; and
- closing said pinhole.

The Patent Office asserts that Bendinelli anticipates claims 1-3, 5, 8, 12, 15-17, 21, 25, and 26. Appellant respectfully disagrees. Bendinelli does not teach the claimed communications between the firewall and the firewall controller. In particular, Bendinelli does not teach sending a request message from a firewall controller to a firewall requesting that a pinhole be opened and closed. Figures 15A and 15B, as well as the supporting specification, of Bendinelli use an alternate proxy, referenced as a proxy module 1520, to provide an alternate path into the private network. There is no direct communications between a firewall controller and a firewall. Instead, the proxy module 1520 coordinates with the respective gateways, 1510 or 1530, to bypass the respective firewalls, 1590 or 1591. Bendinelli specifically states that proxy module 1520 is used as a hairpin, thereby "...bypassing the firewall 1591 of the second gateway 1530." (Bendinelli, col. 39, lines 1-7). Similar operation is provided for the embodiment illustrated in Figure 15B of Bendinelli.

Importantly, Bendinelli fails to disclose a firewall controller sending requests to a firewall to open and close pinholes through the firewall. Requirements for anticipation are strict, and Bendinelli fails to anticipate independent claims 1, 8, 12, 15, 16, 21, and 25-27. Further, Bendinelli actually teaches away from the concepts of the present invention. In fact, the present invention is trying to overcome the limitations of using proxies, such as those recommended by Bendinelli.

In the Final Office Action, the Patent Office responds by quoting col. 37, line 61 through col. 38, line 5 of Bendinelli:

If both the originating gateway (e.g., the first gateway 650) and the destination gateway (e.g., the second gateway 651) are not accessible behind firewalls (not shown) (steps 1330 and 1390), a direct tunnel between the originating gateway and the destination gateway may not be possible because the firewall may hide the real or public IP addresses of the originating gateway and destination gateway, respectively. As a result, the network operations center 610 may enable at the proxy module 613 a proxy (also referred to herein as a “Hairpin”) (step 1391) to enable a tunnel between the first gateway and the second gateway 651 through the proxy.

The Patent Office also cites to col. 36, lines 1-67, and col. 37, line 1 through col. 38, line 30 of Bendinelli. These passages, as well as the above quoted portion of Bendinelli confirm that Bendinelli uses a proxy, as discouraged by the present invention (see Specification, page 3, lines 3-7), and not the claimed firewall controller. Thus, Bendinelli fails to teach a firewall controller sending requests to a firewall to open and close pinholes through the firewall, as required by the present invention. Claims 1-3, 5, 8, 12, 15-17, 21, 25, and 26 all contain limitations regarding sending requests from a firewall controller to a firewall to open and close pinholes through the firewall and are thus allowable since Bendinelli fails to teach each and every element of these claims.

Claim 15 and 26 are further allowable because claims 15 and 26 recite that the firewall is responsive to a media gateway controller and that a request message is received from the media gateway controller to open and close a pinhole in the firewall. The Patent Office admits that Bendinelli does not teach a media gateway controller to control the firewall (Final Office Action mailed June 7, 2006, page 5). Since Bendinelli does not teach a media gateway controller to control the firewall, claims 15 and 26 are patentable for this additional reason.

E. Claims 4, 6, 9, 11, 13, 18, 20, 22, 24, and 27-29 Are Non-Obvious

Claims 4, 6, 9, 11, 13, 18, 20, 22, 24, and 27-29 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Bendinelli in view of Kimchi et al. (hereinafter “Kimchi”). For the Patent Office to establish *prima facie* obviousness, the Patent Office must show where each and every element of the claim is taught or suggested in the combination of references. MPEP § 2143.03. If the Patent Office cannot establish obviousness, then the claims are allowable.

Claims 4, 6, 9, 11, 13, 18, 20, 22, 24, and 27-29 all depend directly or indirectly from one of the independent claims and thus contain the same limitations as their respective independent claims. Thus, these claims also include the limitation that the firewall controller sends requests to open and close pinholes in the firewall. As indicated above, Bendinelli fails to disclose sending requests from a firewall controller to open and close pinholes within the firewall, as required by the independent claims. Kimchi fails to remedy the deficiencies of Bendinelli with regards to opening and closing pinholes in the firewall. Since Bendinelli and Kimchi fail to teach or suggest all of the elements in the claims, the Patent Office has failed to establish *prima facie* obviousness to support these rejections.

Claims 4, 11, 20, and 24 also include the limitation that the firewall controller is a media gateway controller. Bendinelli fails to disclose a firewall controller being a media gateway controller. The Patent Office admits this on page 6 of the Final Office Action mailed June 7, 2006. Instead, the Patent Office uses a reference to the media gateway control protocol in Kimchi to disclose this element (Final Office Action mailed June 7, 2006, page 3 and page 7). Simply finding a statement that the media gateway control protocol controls media gateways to establish media sessions falls vastly short of the requirement of the Patent Office to show where the element as claimed is specifically taught or suggested. Although Kimchi does disclose a media gateway controller, Kimchi certainly does not teach or suggest using a media gateway controller as a firewall controller that sends requests to open and close pinholes within the firewall, as in the claimed invention. Since Kimchi does not teach or suggest using a media gateway controller as a firewall controller, Kimchi does not teach or suggest the limitation for which it is cited. The element of a firewall controller being a media gateway controller is clearly absent from the combination of Bendinelli and Kimchi. Accordingly, claims 4, 11, 20, and 24 define patentable subject matter for this additional reason.

F. Claims 7, 10, 14, 19, and 23 Are Non-Obvious

Claims 7, 10, 14, 19, and 23 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Beninelli in view of Putzolu. The standards for obviousness are set forth in the above.

Claims 7, 10, 14, 19, and 23 all depend directly or indirectly from one of the independent claims and thus contain the same limitations as their respective independent claims. Thus, these

claims also include the limitation that the firewall controller sends requests to open and close pinholes in the firewall. As indicated above, Bendinelli fails to teach or suggest the broader concept of allowing a firewall controller to control a firewall to open and close pinholes. Putzolu fails to remedy this deficiency. Again, the Patent Office must show where each and every element is taught or suggested in the combination of references. Every element is not found in this combination.

G. Conclusion

Claims 1-3, 5, 8, 12, 15-17, 21, 25, and 26 all contain limitations regarding a firewall controller sending requests to a firewall to open and close pinholes through the firewall. Claims 4, 11, 20, 24, and 26 include the further limitation that the firewall controller is a media gateway controller. Bendinelli does not teach a firewall controller sending requests to a firewall to open and close pinholes through the firewall, as required by the claimed invention. In addition, the Patent Office admits that Bendinelli does not teach where the firewall controller is a media gateway controller. Kimchi discloses media gateway controllers, but does not teach or suggest using media gateway controllers as firewall controllers. Thus, Kimchi does not cure the deficiencies of Bendinelli. Likewise, Putzolu also fails to teach the limitations missing from Bendinelli.

Accordingly, since the references, alone or in combination, fail to teach or suggest each and every element of the claimed invention, pending claims 1-29 are allowable. As such, Appellant requests that the Board reverse the Examiner and instruct the Examiner to allow the claims for these reasons.

Respectfully submitted,

WITHROW & TERRANOVA, P.L.L.C.

By:



John R. Witcher, III
Registration No. 39,877
P.O. Box 1287
Cary, NC 27512
Telephone: (919) 654-4520

Date: January 15, 2007
Attorney Docket: 7000-445

(8) APPENDIX

1. A method of remotely controlling a firewall from a firewall controller in order to permit the flow of packet data through said firewall, the method comprising:
 - sending a request message from a firewall controller to a firewall requesting that a pinhole be opened;
 - opening a pinhole in said firewall;
 - sending a request message from a firewall controller to said firewall requesting that a pinhole be closed; and
 - closing said pinhole.
2. The method of claim 1 further comprising:
 - determining the need for a pinhole in said firewall.
3. The method of claim 2 wherein said step of determining occurs at said firewall controller.
4. The method of claim 3 wherein said firewall controller is a media gateway controller.
5. The method of claim 1 further including the step of determining the need for a pinhole prior to sending a request that a pinhole be opened.
6. The method of claim 1 wherein said request messages are formatted in the H.248 protocol.
7. The method of claim 1 wherein said request messages are formatted in the common open policy services (COPS) protocol.
8. A firewall controller for permitting the flow of packet data, said firewall controller comprising:
 - means for determining a need for a pinhole in a firewall;

means for sending a request message to said firewall requesting that a pinhole be opened in said firewall; and

means for sending a request message to said firewall requesting that said pinhole be closed in said firewall.

9. The firewall controller of claim 8 wherein said request messages are formatted in the H.248 protocol.

10. The firewall controller of claim 8 wherein said request messages are formatted in the common open policy services (COPS) protocol.

11. The firewall controller of claim 8 wherein said firewall controller is a media gateway controller.

12. A firewall responsive to a firewall controller for permitting the flow of packet data, said firewall comprising:

means for receiving a request message from said firewall controller requesting that a pinhole be opened in said firewall;

means for opening a pinhole in said firewall;

means for receiving a request message from said firewall controller requesting that said pinhole be closed in said firewall; and

means for closing said pinhole in said firewall.

13. The firewall of claim 12 wherein said request messages are formatted in the H.248 protocol.

14. The firewall of claim 12 wherein said request messages are formatted in the common open policy services (COPS) protocol.

15. A firewall responsive to a media gateway controller for permitting the flow of packet data, said firewall comprising:

means for receiving a request message from said media gateway controller requesting that a pinhole be opened in said firewall;

means for opening a pinhole in said firewall;

means for receiving a request message from said media gateway controller requesting that said pinhole be closed in said firewall; and

means for closing said pinhole in said firewall.

16. A computer program product for remotely controlling a firewall from a firewall controller in order to permit the flow of packet data through said firewall, the computer program product having a medium with a computer program embodied thereon, the computer program product comprising:

computer program code in said firewall controller for sending a request message to said firewall requesting that a pinhole be opened; and

computer program code in said firewall for opening a pinhole;

computer program code in said firewall controller for sending a request message to said firewall requesting that said pinhole be closed; and

computer program code in said firewall for closing said pin hole.

17. The computer program product of claim 16 further comprising:

computer program code in said firewall controller for determining the need for a pinhole in said firewall.

18. The computer program product of claim 16 wherein said request messages are formatted in the H.248 protocol.

19. The computer program product of claim 16 wherein said request messages are formatted in the common open policy services (COPS) protocol.

20. The computer program product of claim 17 wherein said firewall controller is a media gateway controller.

21. A computer program product in a firewall controller, said firewall controller operative with a firewall, the computer program product having a medium with a computer program embodied thereon, the computer program product comprising:
- computer program code for determining the need for a pinhole in said firewall;
 - computer program code for sending a request message to said firewall requesting that a pinhole be opened in said firewall; and
 - computer program code for sending a request message to said firewall requesting that said pinhole be closed in said firewall.
22. The computer program product of claim 21 wherein said request messages are formatted in the H.248 protocol.
23. The computer program product of claim 21 wherein said request messages are formatted in the common open policy services (COPS) protocol.
24. The computer program product of claim 21 wherein said firewall controller is a media gateway controller.
25. A computer program product in a firewall, said firewall responsive to a firewall controller, the computer program product having a medium with a computer program embodied thereon, the computer program product comprising:
- computer program code for receiving a request message from said firewall controller requesting that a pinhole be opened in said firewall;
 - computer program code for opening a pinhole in said firewall;
 - computer program code for receiving a request message from said firewall controller requesting that said pinhole be closed in said firewall; and
 - computer program code for closing said pinhole in said firewall.
26. A computer program product in a firewall, said firewall responsive to a media gateway controller, the computer program product having a medium with a computer program embodied thereon, the computer program product comprising:

computer program code for receiving a request message from said media gateway controller requesting that a pinhole be opened in said firewall;
computer program code for opening a pinhole in said firewall;
computer program code for receiving a request message from said media gateway controller requesting that said pinhole be closed in said firewall; and
computer program code for closing said pinhole in said firewall.

27. A computer system for remotely controlling a firewall from a firewall controller comprising:

a firewall operatively connected to a private computer network and at least one external computer network;

a firewall controller operatively connected to said firewall for remotely instructing said firewall to open and close pinholes in said firewall.

28. The computer system of claim 27 wherein said firewall controller is a media gateway controller acting as a call server to a VoIP telephony network.

29. The computer system of claim 28 wherein said media gateway controller instructs said firewall to open and close pinholes in said firewall such that media gateway endpoints within said private network can communicate with media gateway endpoints outside said private network on a per call basis.

(9) EVIDENCE APPENDIX

Appellant relies on no evidence, thus this appendix is not applicable.

(10) RELATED PROCEEDINGS APPENDIX

As there are no related proceedings, this appendix is not applicable.